Kevin Staggs
August 18, 2016

CYBER SECURITY AND RESILIENCY

Honeywell

Speaker information

- Kevin Staggs, CISSP, CSSLP
- Senior Engineering Fellow
- 40 years experience with ICS systems
- 20+ years experience with ICS cyber security
- Currently a consultant to Honeywell businesses for:
  - Product security
  - Security development lifecycle processes
  - Cyber security training
  - Mentoring business cyber security leaders
  - Advanced cyber security testing
- Co-chair of ISA-99 WG4
  - IEC-62443 Standards
- Founding member of ISA Security Compliance Institute (ISCI)

Honeywell

ICS History

- Digital ICS systems introduced as closed proprietary systems
- HMI and Servers transition to COTS
  - Microsoft provided good guidance for deploying Windows NT securely
  - Not all ICS vendors followed recommentations
- ICS networks migrated to COTS networks
- ICS controllers migrated to COTS networks
  - Simply moved proprietary communications to run on Ethernet networks
  - Serial communications protocols migrated to Ethernet
    - Protocols lack any form of cyber security
  - ICS controller reliability (resiliency) begins to decline
    - Easy to DoS controllers
- ICS cyber security journey begins
  - ISA-99 formed
  - Wurldtech Industrial Device Certification created
  - ISA Security Compliance Institute (ICSI) formed
- Stuxnet

Honeywell

It’s more than ICS

- Digital ICS systems are cyber-physical systems
- Other types of cyber-physical systems
  - Building Control Systems
    - HVAC
    - Access Control
    - Energy Management
    - Video System
  - Aircraft Control Systems
  - Medical Systems
  - Vehicle Control Systems

Honeywell

Cyber-physical systems have the same risks

- Compromise of most modern cyber-physical control system could result in any or all of the following situations:
  - endangerment of public or employee safety
  - environmental protection
  - loss of public confidence
  - violation of regulatory requirements
  - loss of proprietary or confidential information
  - economic loss
  - impact on entity, local, state, or national security
- Same approach to cyber security risk management should apply
  - NIST Cybersecurity Framework
  - ISA-62443 Standards
  - ISASecure Certification

Table 1: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Honeywell

The Basics of ISA-62443

- General Concepts
- Fundamental Concepts

Copyright © ISA

Honeywell

General Concepts

- Security Context
- Security Objectives
- Least Privilege
- Defense in Depth
- Threat-Risk Assessment
- Policies and Procedures

Source: ISA-62443-1-1, 2nd Edition (Under development)

Honeywell

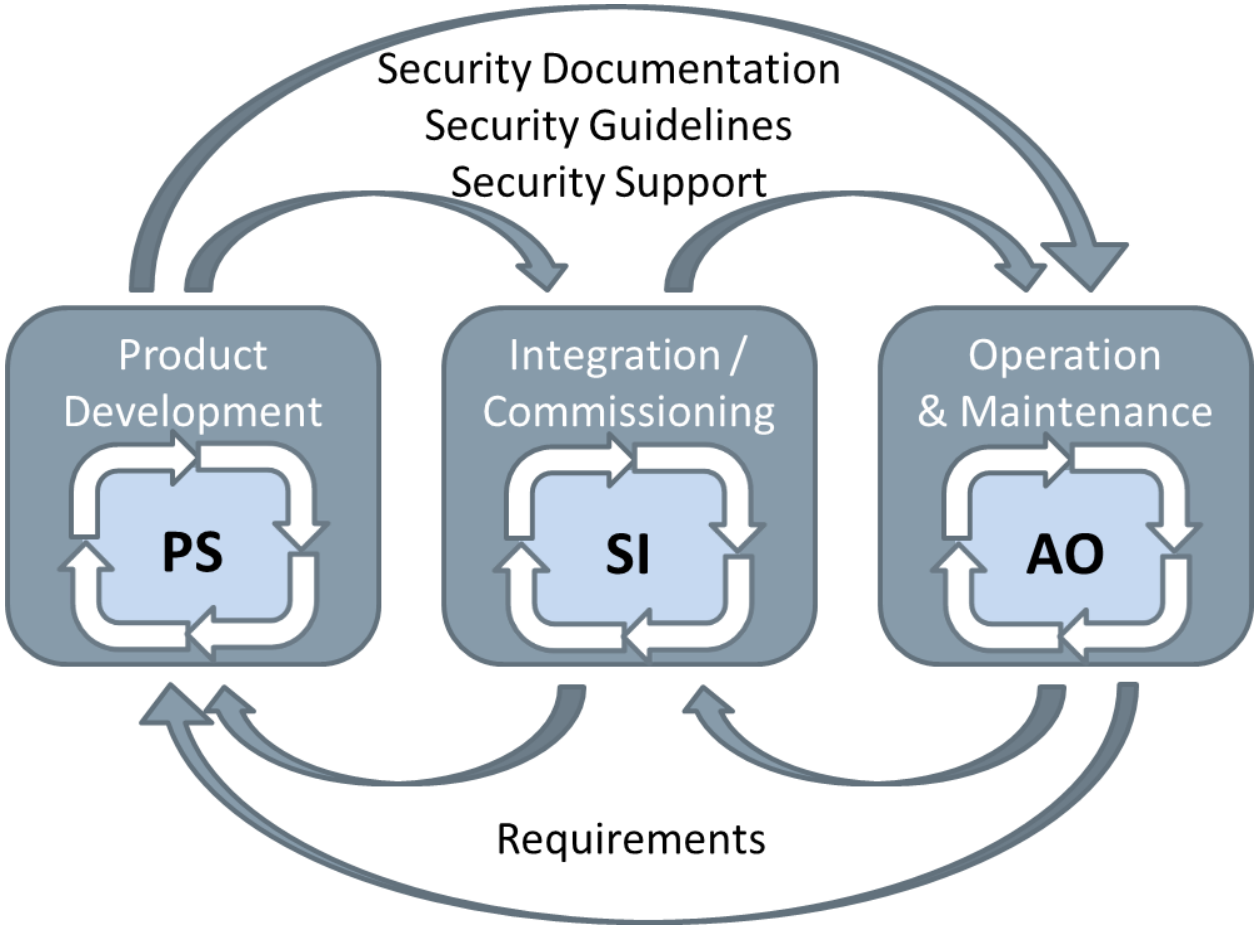
Fundamental Concepts

- Security Life Cycle
- Zones and Conduits
- Security Levels
- Foundational Requirements
- Program Maturity
- Safety and Security

Source: ISA-62443-1-1, 2nd Edition (Under development)

Honeywell

Security Life Cycle



Source: ISA-62443-1-1, 2nd Edition (Under development)

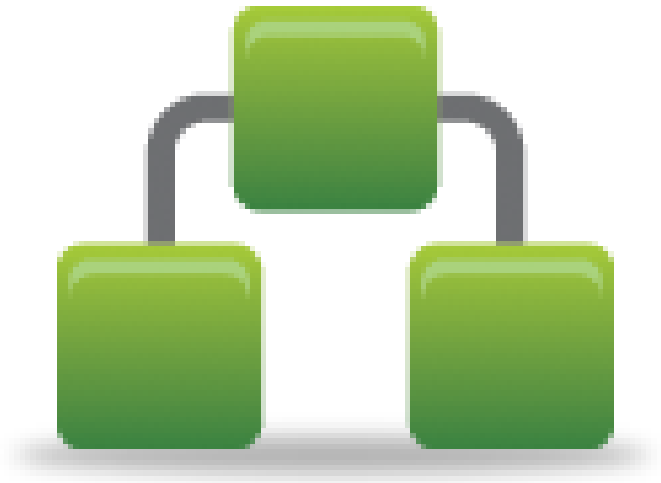
Copyright © ISA

Honeywell

Zones and Conduits

A network & system segmentation technique:

- Prevents the spread of an incident
- Provides a front-line set of defenses
- The basis for risk assessment in system design



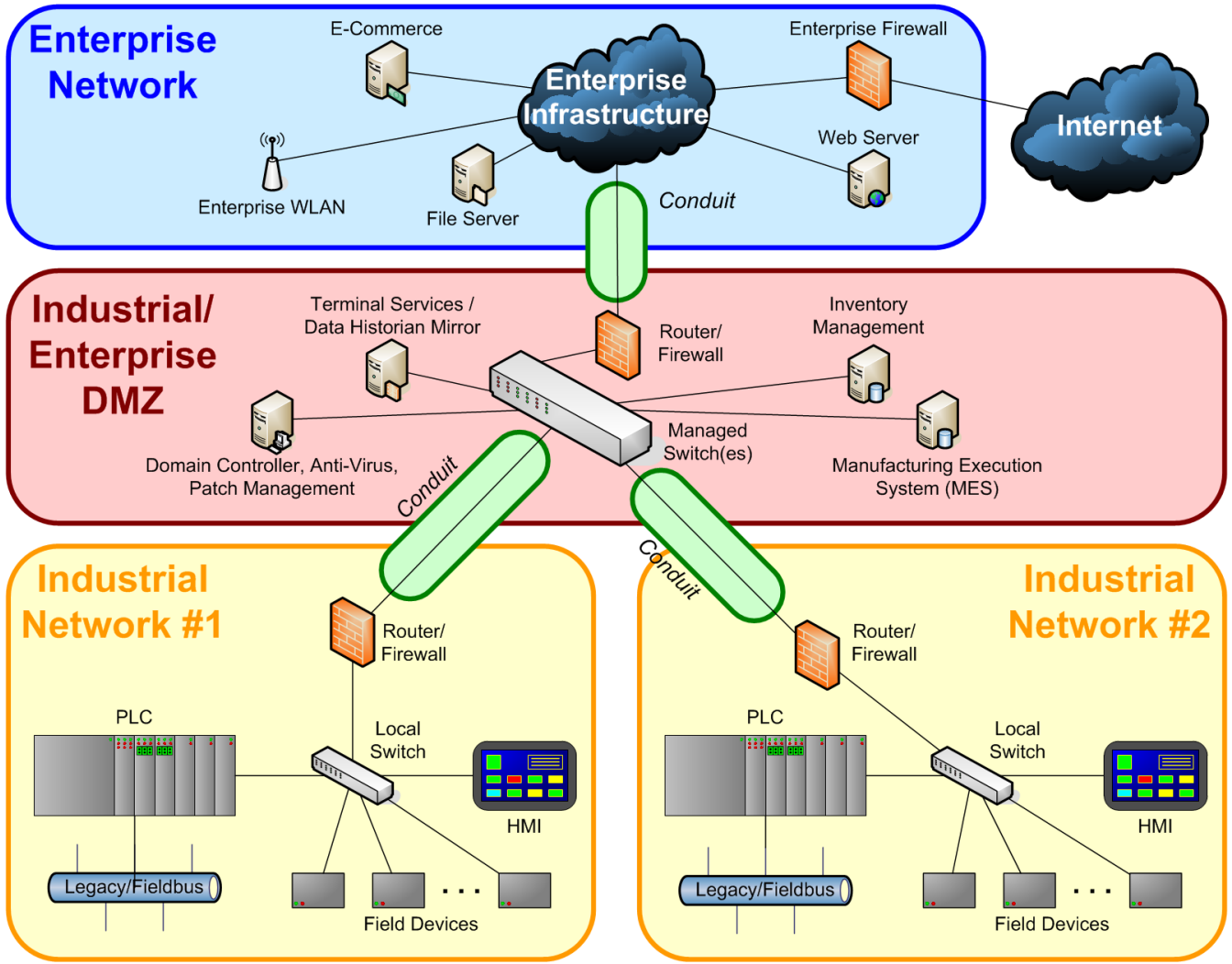
Copyright © ISA

Honeywell

System Segmentation

- A process to understand:
  - How different systems interact
  - Where information flows between systems
  - What form that information takes
  - What devices communicate
  - How fast/often those devices communicate
  - The security differences between system components
- Technology helps, but architecture is more important

Example



Copyright © ISA

Honeywell

Security Levels

Foundational Requirements

- FR 1 – Identification & authentication control
- FR 2 – Use control
- FR 3 – System integrity
- FR 4 – Data confidentiality
- FR 5 – Restricted data flow
- FR 6 – Timely response to events
- FR 7 – Resource availability

Program Maturity

- A means of assessing capability
- Similar in concept to Capability Maturity Models
  - e.g., SEI-CMM
- An evolving concept in the standards
  - Applicability to IACS-SMS

Safety and Security

- Safety is much of the “raison d’etre” for security
  - Presenting consequences
- Much to be learned from the Security community
- Collaboration
  - ISA99-ISA84 joint efforts
  - ISA Safety and Security Division

Honeywell

Fundamental Concepts Status

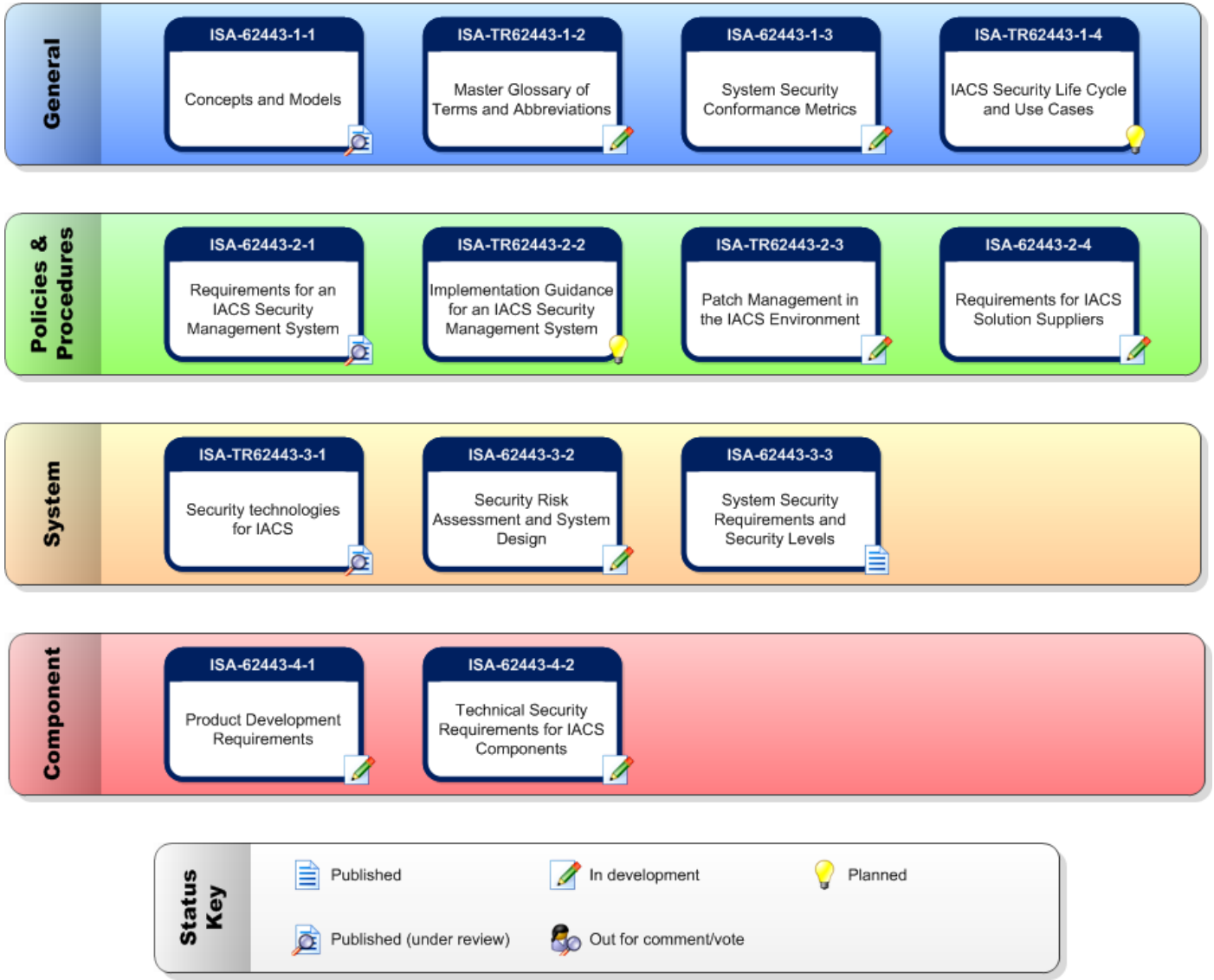
- ✓ Security Life Cycle
- ✓ Zones and Conduits
- → Security Levels
- ✓ Foundational Requirements
- → Program Maturity
- → Safety and Security

Honeywell

Work Products

Honeywell

The ISA-62443/IEC 62443 Series



Copyright © ISA

Honeywell

General Information

- ISA-62443-1-1
  - Concepts and Models
- ISA-TR62443-1-2
  - Master Glossary
- ISA-TR62443-1-3
  - Metrics
- ISA-TR62443-1-4
  - Lifecycle & Use Cases

Policies and Procedures

- ISA-62443-2-1
  - Security Management System
- ISA-TR62443-2-2
  - Implementation Guidance
- ISA-TR62443-2-3
  - Patch Management
- ISA-62443-2-4
  - Requirements for Suppliers

System Requirements

- ISA-TR62443-3-1
  - Security Technologies
- ISA-62443-3-2
  - Risk Assessment and Design
- ISA-62443-3-3
  - System Requirements

Honeywell

Component Requirements

- ISA-62443-4-1
  - Product Development
- ISA-62443-4-2
  - Technical Component

ISA Security Compliance Institute (ISCI)

Honeywell

About ISCI

Organization

Consortium of Asset Owners, Suppliers, and Industry Organizations formed in 2007 under the ISA Automation Standards Compliance Institute (ASCI):

Mission

Establish a set of well-engineered specifications and processes for the testing and certification of industrial automation and control systems products

Decrease the time, cost, and risk of developing, acquiring, and deploying control systems by establishing a collaborative industry-based program among asset owners, suppliers, and other stakeholders

Honeywell

Internationally Accredited Conformance Scheme

ISASecure certification programs are accredited as an ISO/IEC Guide 65 conformance scheme and ISO/IEC 17025 lab operations by ANSI/ACLASS.

- Provides global recognition for ISASecure certification
- Independent CB accreditation by ANSI/ACLASS and other global Accreditation Bodies such as JAB or UKAS
- ISASecure can scale on a global basis
- Ensures certification process is open, fair, credible, and robust.
- MOU's with AB's for ISASecure

Honeywell

Objective of ISASecure

- One set of certification criteria
- One certification test/assessment
- One globally recognized mark

Economically efficient for both suppliers and asset owners

Honeywell

ISASecure™ Security Development Lifecycle Assurance (SDLA)

Honeywell

SDLA Overview

- Certification that the supplier's:
  - product development work process includes security considerations throughout the lifecycle. (Organization process certification)
  - Process meets the requirements of ISA/IEC-62443-4-1
- Based on several industry-recognized security development lifecycle processes

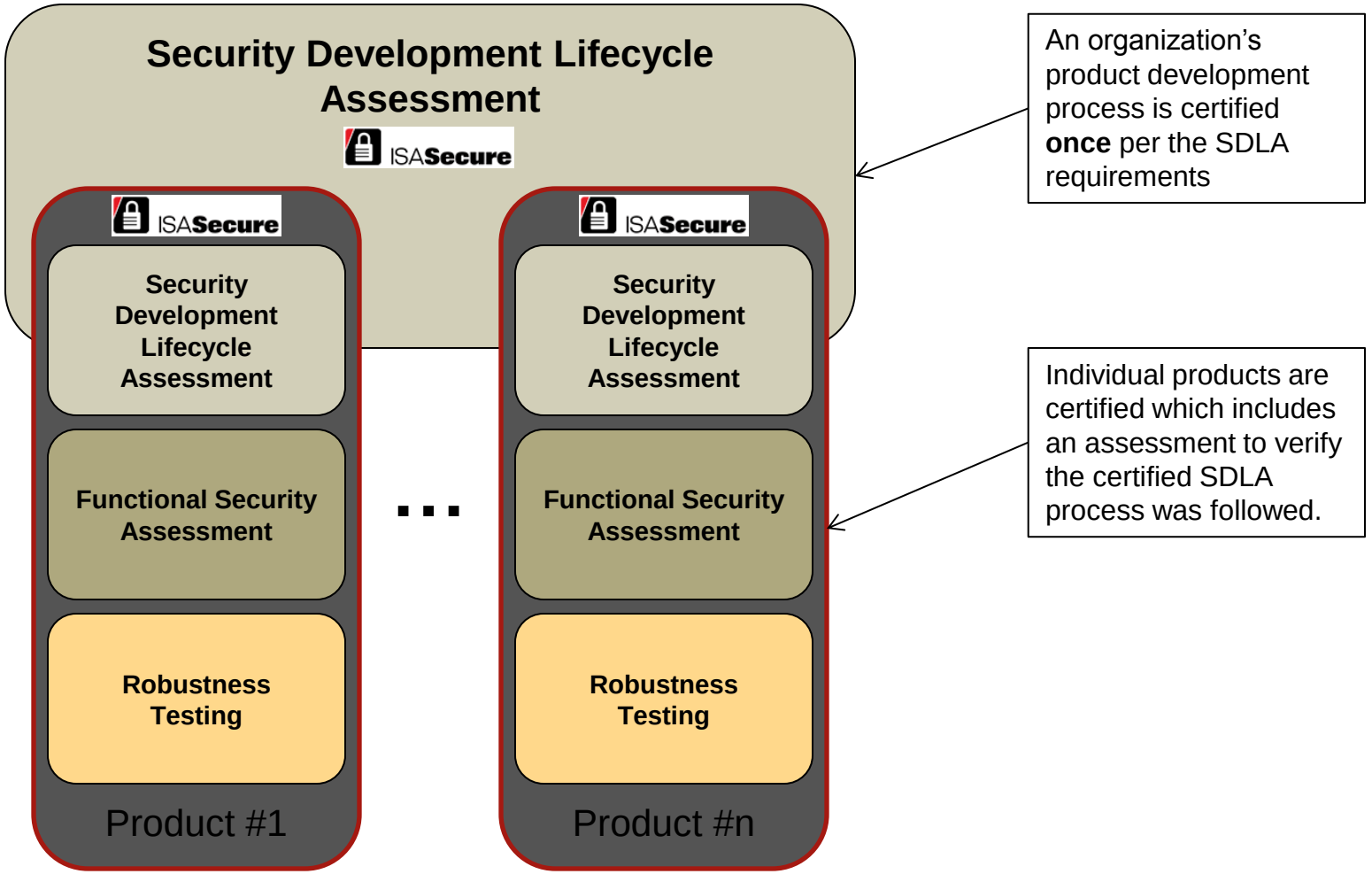
Honeywell

SDLA Phases

1. Security Management Process
2. Security Requirements Specification
3. Security Architecture Design
4. Security Risk Assessment (Threat Model)
5. Detailed Software Design
6. Document Security Guidelines
7. Module Implementation & Verification
8. Security Integration Testing
9. Security Process Verification
10. Security Response Planning
11. Security Validation Testing
12. Security Response Execution

Honeywell

Multiple Product Certification



Honeywell

ISASecure™ Embedded Device Security Assurance (EDSA)

Honeywell

EDSA Overview

- Certification that the supplier's product:
  - is robust against network attacks and is free from known security vulnerabilities
  - Meets requirements of ISA/IEC-62443-4-2 for embedded devices
  - Is developed following a robust security development lifecycle

Honeywell

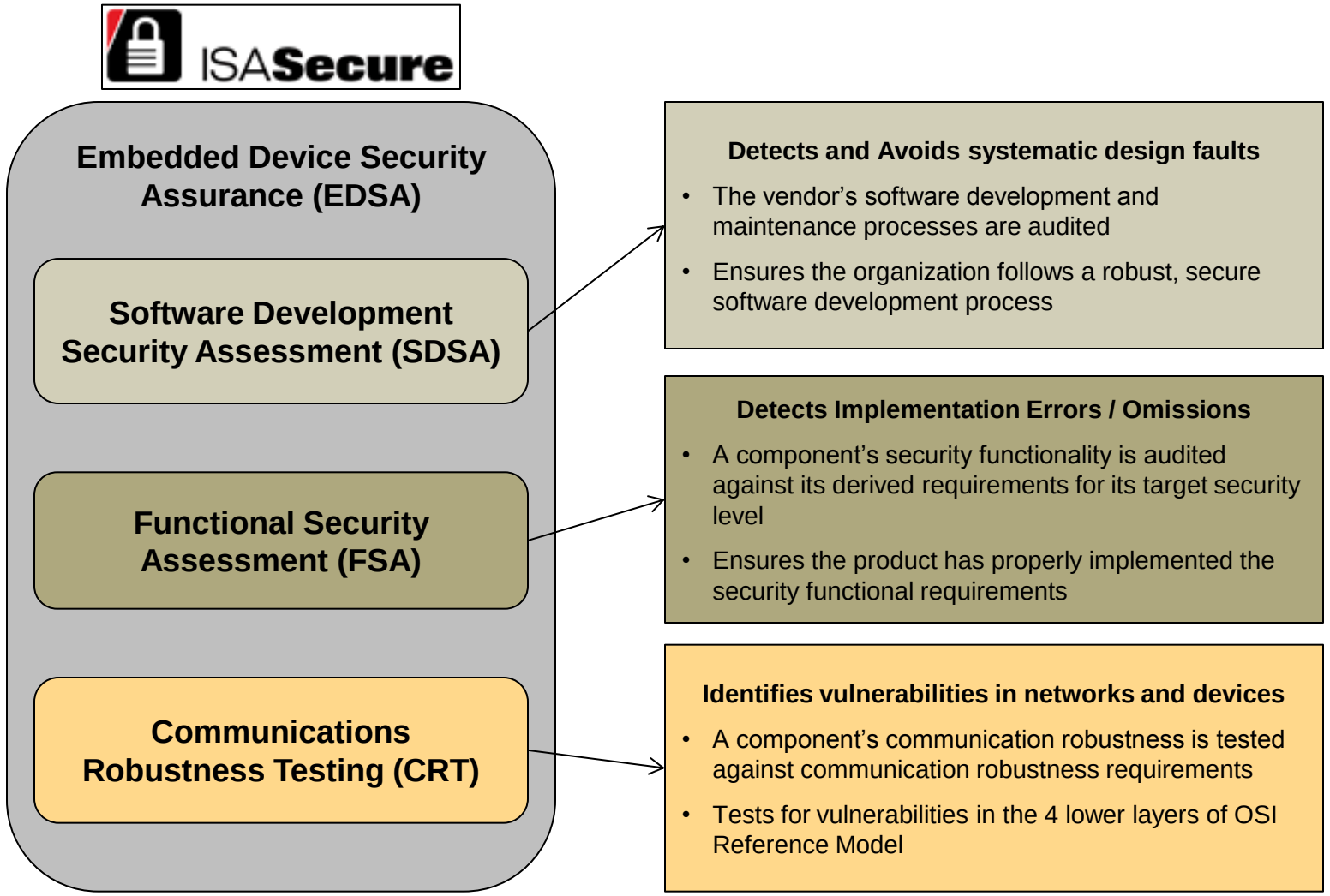
What is an Embedded Device?

Special purpose device running embedded software designed to directly monitor, control or actuate an industrial process, examples:

- Programmable Logic Controller (PLC)
- Distributed Control System (DCS) controller
- Safety Logic Solver
- Programmable Automation Controller (PAC)
- Intelligent Electronic Device (IED)
- Digital Protective Relay
- Smart Motor Starter/Controller
- SCADA Controller
- Remote Terminal Unit (RTU)
- Turbine controller
- Vibration monitoring controller
- Compressor controller

Honeywell

ISASecure EDSA Certification Program



Honeywell

ISASecure™ System Security Assurance (SSA)

Honeywell

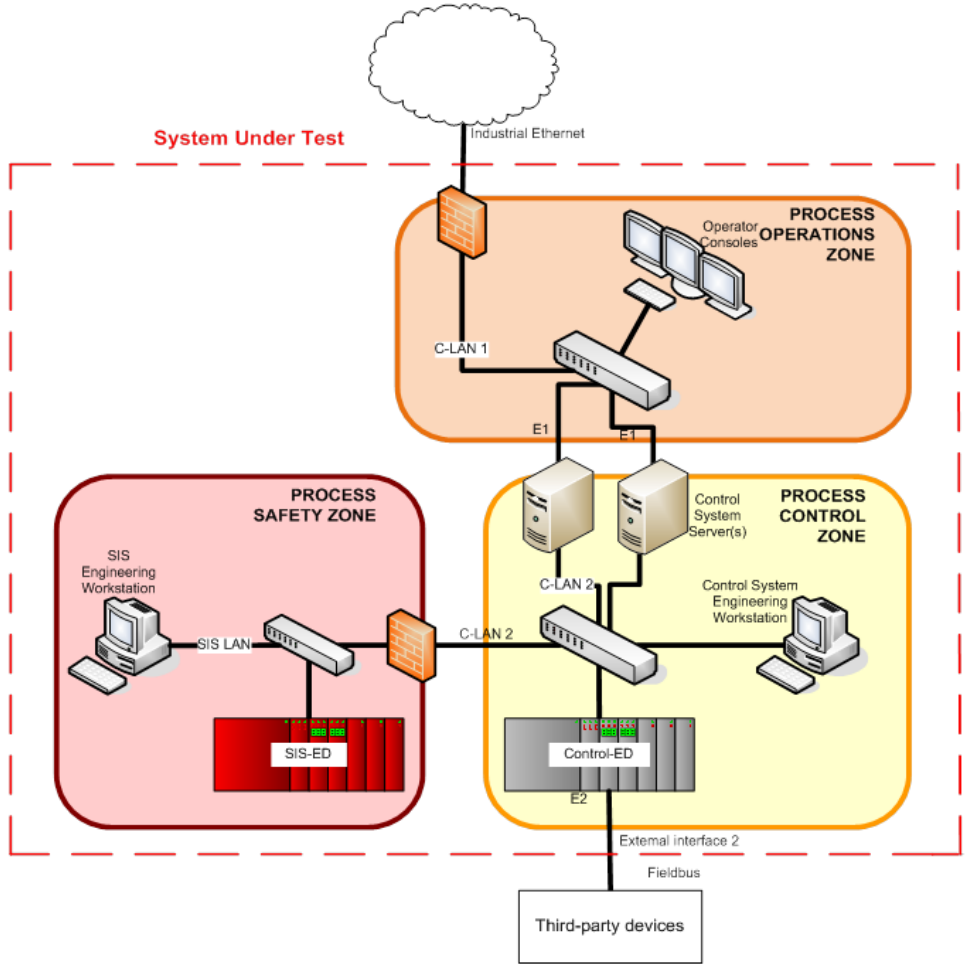
SSA Overview

- Certification that the supplier's product:
  - is robust against network attacks and is free from known security vulnerabilities
  - Meets requirements of ISA/IEC-62443-3-3
  - Is developed following a robust security development lifecycle

Honeywell

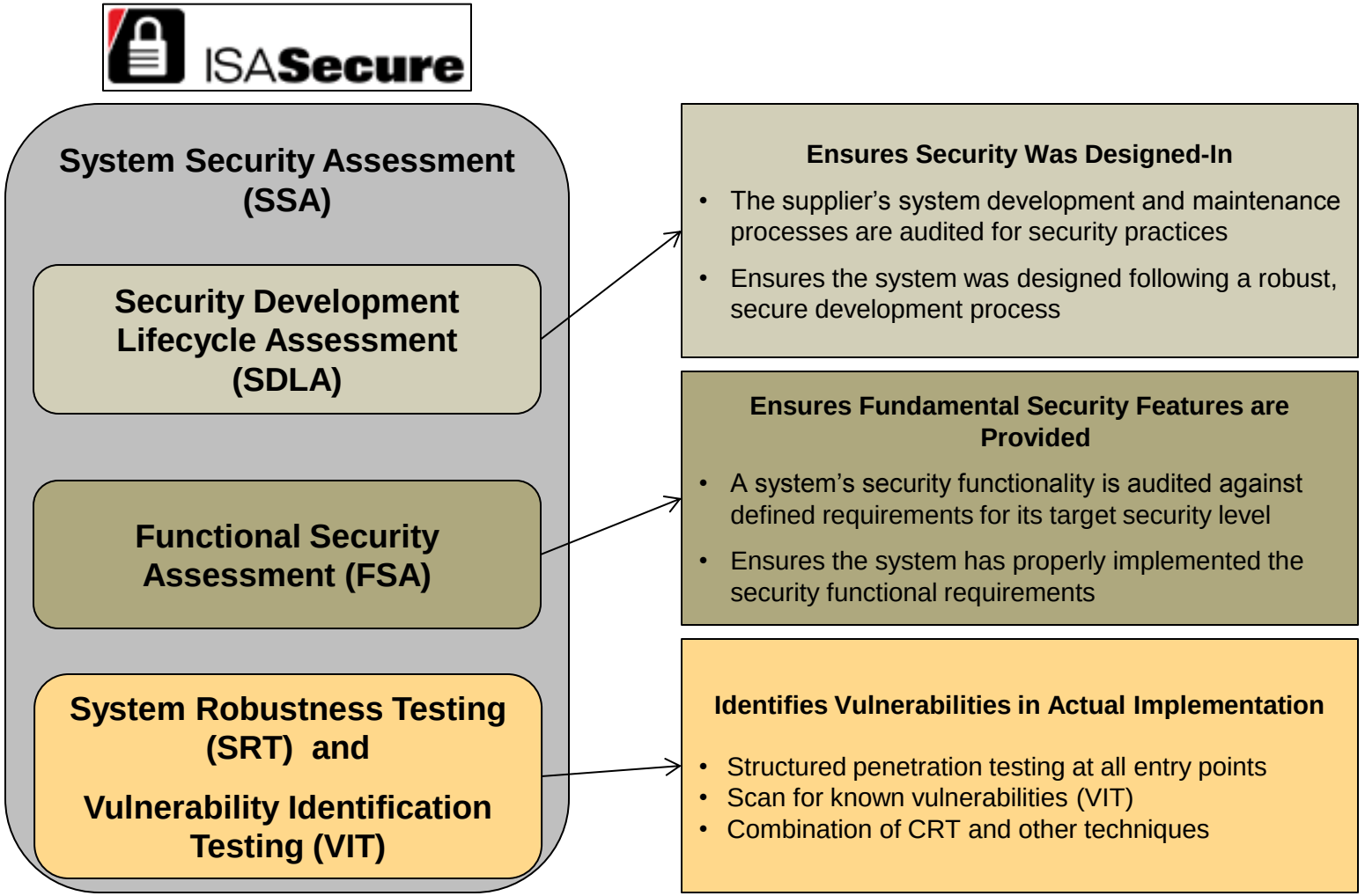
What is a “System” ?

- Industrial Control System (ICS) or SCADA system
- Available from a single supplier
- Supported by a single supplier
- Components are integrated into a single system
- May consist of multiple Security Zones
- Can be identified by a product name and version
- Off the shelf; not site or project engineered yet



Honeywell

ISASecure SSA Certification Program



Honeywell

SSA System Robustness Test

- Asset Discovery Scan
  - scan to discover the components on the network
- Communications Robustness Test
  - verify that essential functions continue to operate under high network load and malformed packets
- Network Stress Test
  - verify that essential functions continue to operate under high network load
- Vulnerability Identification Test
  - scan all components for the presence of known vulnerabilities (using Nessus)
  - based on National Vulnerability Database

Honeywell

Conclusion

- A robust control system cyber security management system
  - Is established using a well defined cyber security framework such as the NIST Cybersecurity Framework
    - Using ISA-62443 as the basis for control system security
  - Involves everyone in the control system lifecycle
    - Owner/Operators
    - System integrators and service providers
    - System and component vendors
  - Is validated to meet cyber security requirements
    - ISASecure

Honeywell